XIAO ZHANG

Phone: +1 (434) 466 7098 Email: xiaozhanguva2015@gmail.com
Homepage: https://xiao-zhang.net Github: https://github.com/xiaozhanguva
Google Scholar: https://scholar.google.com/citations?user=L-lz7CUAAAAJ&hl=en

EDUCATION

Ph.D. in Computer Science *2017 - Present*
Department of Computer Science, University of Virginia, Charlottesville, VA, USA

Master of Science in Statistics *2015 - 2017*
Department of Statistics, University of Virginia, Charlottesville, VA, USA

Bachelor of Science in Mathematics *2011 - 2015*
Department of Mathematical Science, Tsinghua University, Beijing, China

RESEARCH INTERESTS

Machine Learning: adversarial machine learning, statistical machine learning, deep learning
Optimization: convex/non-convex optimization, low-rank matrix recovery

PROFESSIONAL EXPERIENCES

Robert Bosch LLC, Pittsburgh, PA, USA *Jun 2020 - Oct 2020*
Machine Learning Research Intern
Mentor: Anit Kumar Sahu
Project: Building efficient adversarially robust classification models using meta learning techniques

CONFERENCE PUBLICATIONS

* denotes equal contribution.

1. **Xiao Zhang** and David Evans
Understanding Intrinsic Robustness using Label Uncertainty
In the Tenth International Conference on Learning Representations (ICLR 2022)
[PDF] [Link] [ArXiv]

2. Jack Prescott, **Xiao Zhang**, and David Evans
Improved Estimation of Concentration under ℓ_p-norm Distance Metrics using Half Spaces
In the Ninth International Conference on Learning Representations (ICLR 2021)
[Acceptance rate : 28.7%] [PDF] [Link] [ArXiv]

3. Sicheng Zhu*, **Xiao Zhang***, and David Evans
Learning Adversarially Robust Representations via Worst-Case Mutual Information Maximization.
In the Thirty-seventh International Conference on Machine Learning (ICML 2020)
[Acceptance rate : 21.8%] [PDF] [Link] [ArXiv]

4. **Xiao Zhang***, Jinghui Chen*, Quanquan Gu and David Evans
Understanding the Intrinsic Robustness of Image Distributions using Conditional Generative Models.
In the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS 2020)
[PDF] [Link] [ArXiv]

5. Saeed Mahloujifar*, **Xiao Zhang***, Mohammad Mahmoody and David Evans
Empirically Measuring Concentration: Fundamental Limits to Intrinsic Robustness.
In the Thirty-third Conference on Neural Information Processing Systems (NeurIPS 2019)
[Spotlight, 164/6743 (2.97%)] [PDF] [Link] [ArXiv]

6. **Xiao Zhang** and David Evans
   Cost-Sensitive Robustness against Adversarial Examples.
   In the Seventh International Conference on Learning Representations (ICLR 2019)
   [Acceptance rate : 31.4%] [PDF] [Link] [ArXiv]

7. **Xiao Zhang***, Yaodong Yu*, Lingxiao Wang* and Quanquan Gu
   Learning One-hidden-layer ReLU Networks via Gradient Descent.
   In the 22nd International Conference on Artificial Intelligence and Statistics (AISTATS 2019)
   [Acceptance rate : 32.4%] [PDF] [Link] [ArXiv]

8. **Xiao Zhang***, Simon S. Du* and Quanquan Gu
   Fast and Sample Efficient Inductive Matrix Completion via Multi-Phase Procrustes Flow.
   In the Thirty-fifth International Conference on Machine Learning (ICML 2018)
   [Acceptance rate : 25.1%] [PDF] [Link] [ArXiv]

9. **Xiao Zhang***, Lingxiao Wang*, Yaodong Yu and Quanquan Gu
   A Primal-Dual Analysis of Global Optimality in Nonconvex Low-Rank Matrix Recovery
   In the Thirty-fifth International Conference on Machine Learning (ICML 2018)
   [Acceptance rate : 25.1%] [PDF] [Link]

10. **Xiao Zhang***, Lingxiao Wang* and Quanquan Gu
    A Unified Framework for Nonconvex Low-Rank plus Sparse Matrix Recovery
    In the 21st International Conference on Artificial Intelligence and Statistics (AISTATS 2018)
    [Acceptance rate : 33.2%] [PDF] [Link] [ArXiv]

11. Lingxiao Wang*, **Xiao Zhang*** and Quanquan Gu
    A Unified Variance Reduction-Based Framework for Nonconvex Low-Rank Matrix Recovery.
    In the Thirty-fourth International Conference on Machine Learning (ICML 2017)
    [Acceptance rate : 25.9%] [PDF] [Link] [ArXiv]

12. Lingxiao Wang*, **Xiao Zhang*** and Quanquan Gu
    A Unified Computational and Statistical Framework for Nonconvex Low-Rank Matrix Estimation.
    In the 20th International Conference on Artificial Intelligence and Statistics (AISTATS 2017)
    [Acceptance rate : 31.7%] [PDF] [Link] [ArXiv]

WORKSHOP PAPERS AND PREPRINTS

1. **Xiao Zhang** and David Evans
   Incorporating Label Uncertainty in Intrinsic Robustness Measures.
   ICLR 2021 Workshop on Security and Safety in Machine Learning Systems

2. Saeed Mahloujifar*, **Xiao Zhang***, Mohammad Mahmoody and David Evans
   Empirically Measuring Concentration: Fundamental Limits to Intrinsic Robustness.
   ICML 2019 Workshops on Uncertainty & Robustness in Deep Learning Workshop and
   ICLR 2019 Workshops on Safe Machine Learning and Debugging Machine Learning Models

3. Jinghui Chen, Lingxiao Wang, **Xiao Zhang** and Quanquan Gu
   Robust Wirtinger Flow for Phase Retrieval with Arbitrary Corruption.
   ArXiv:1704.06256, 2017

TALKS AND PRESENTATIONS

1. Incorporating Label Uncertainty in Intrinsic Robustness Measures
   Workshop on Security and Safety in Machine Learning Systems at ICLR, Online, May 2021
   [Poster]

2. Understanding the Intrinsic Robustness of Image Distributions using Conditional Generative Models
   Artificial Intelligence and Statistics (AISTATS), Online, Aug 2020
   [Slides] [Video]
3. Empirically Measuring Concentration: Fundamental Limits to Intrinsic Robustness
   Neural Information Processing Systems (NeurIPS), Vancouver, Canada, Dec 2019
   [Poster] [Slides] [Video]
4. Cost-Sensitive Robustness against Adversarial Examples
   International Conference on Learning Representations (ICLR), New Orleans, USA, May 2019
   [Poster]
5. Fast and Sample Efficient Inductive Matrix Completion via Multi-Phase Procrustes Flow
   International Conference on Machine Learning (ICML), Stockholm, Sweden, Jul 2018
   [Poster] [Slides] [Video]
6. A Unified Framework for Nonconvex Low-Rank plus Sparse Matrix Recovery
   Artificial Intelligence and Statistics (AISTATS), Lanzarote, Canary Islands, Apr 2018
   [Poster]
7. A Unified Variance Reduction-Based Framework for Nonconvex Low-Rank Matrix Recovery
   International Conference on Machine Learning (ICML), Sydney, Australia, Aug 2017
   [Poster] [Slides] [Video]
8. A Unified Computational and Statistical Framework for Nonconvex Low-Rank Matrix Estimation
   Artificial Intelligence and Statistics (AISTATS), Ft. Lauderdale, Florida, Apr 2017
   [Poster]

PROFESSIONAL SERVICES

Journal Reviewer: Machine Learning (MLJ), Advances in Computational Mathematics (ACOM)

Conference Reviewer: NeurIPS 2020, Neurips 2021, AISTATS 2021, ICLR 2021, ICLR 2022

Student Travel Award: ICML 2017, ICML 2018, ICLR 2019, NeurIPS 2019

MENTORING EXPERIENCES

Sicheng Zhu (Visiting scholar at UVA, paper in ICML 2020, now a CS PhD student at UMD)

Jack Prescott (Undergraduate student at UVA, paper in ICLR 2021)

TEACHING EXPERIENCES

Teaching Assistant, Department of Computer Science, University of Virginia

CS3102: Theory of Computation *2019 fall*

CS6501: Optimization for Machine Learning *2017 fall*

CS2102: Discrete Math *2017 fall*

Teaching Assistant, Department of Statistics, University of Virginia

STAT2120: Introduction to Statistical Science *2016 fall, 2017 spring*